INTERNATIONAL RESEARCH JOURNAL
OF
ENGINEERING & APPLIED SCIENCES

ISSN: 2322-0821(O)
ISSN: 2394-9910(P)

VOLUME 10 ISSUE 2
Apr 2022 - June 2022

www.irjeas.org

A PRIVACY-PRESERVING METHOD FOR SMART GRID DATA USING SWARM INTELLIGENCE ALGORITHM

*Mukesh Kumar[1], Puneet Jain[2], Ajay Kumar[3]

[1]*P.G. Scholar, Electrical Engineering Dept., Adesh Institute of Engineering & Technology, Faridkot, Punjab, India.* er.mukesh531@gmail.com

[2]*Assistant Professor, Electrical Engineering Dept., Adesh Institute of Engineering & Technology, Faridkot, Punjab, India.* puneetjain988@gmail.com

[3]*Ph.D. Scholar, Electronics and Communication Dept., Thapar Institute of Engineering & Technology, Patiala, Punjab, India.* er.ajay.thapar@gmail.com

**Corresponding Author*

Abstract - Users' electricity use may be shared nearly instantly with utilities companies on the smart grid due to Smart Meters (SMs). The data is communicated between individuals in the company, which has prompted privacy issues. In this paper, a privacy-preserving method for smart meter data is designed using a swarm intelligence algorithm. In the swarm intelligence algorithm, JAYA algorithm is taken under consideration and deployed for key generation in the planned method. After that, an XOR operation was performed between the smart meter sensitive data and key generated using a JAYA algorithm for encryption purposes. In MATLAB, numerous performance metrics are computed for the planned technique's performance evaluation. From Simulation results it is clear that the planned method gives better results as compared to the previous methods.

.

Keywords - Encryption, JAYA Algorithm, Privacy-Preserving Method, Security, Smart Grid, Smart Meter, Swarm Intelligence Algorithm.

Manuscript Received: 24 Mar 2022, Accepted: 25 May 2022
DOI – 10.55083/irjeas.2022.v10i2006

1. Introduction

The term "smart grid" refers to the combination of information and communications technologies (ICT) with the conventional power system. To be considered smart, a smart grid must be capable of two-way communication among the various entities that make up the grid. Energy production and consumption may be monitored and controlled more effectively thanks to this method of improved management. As a whole, the smart grid is meant to accomplish the following goals [1]:

- Increased reliance on eco-friendly and renewable energy sources.
- Billing by use of precise measurement and management.
- Energy consumption balancing
- Communication between stakeholders must be two-way.
- Increasing the ability to withstand assaults by malicious users.
- Increased resiliency due to decentralized control.
- Effective use of resources to boost productivity

In spite of the advantages of the smart grid, the two-way connection enables the gathering of fine-

International Research Journal of Engineering & Applied Sciences, IRJEAS
www.irjeas.org, ISSN(O): 2322-0821, ISSN(P): 2394-9910, Volume 10 Issue 2, Apr-Jun 2022, Page 23-32

grained information about user usage via the smart metre. Due to the fact that the information obtained may be used to infer user patterns, appliance categories, and overall energy use, this poses a significant risk of privacy violations. The protection of personal information is thus critical in a smart grid setting. Smart grid privacy and security may be preserved by a number of different strategies that have been put out in the literature. It's practically impossible to maintain privacy effectively without security since the two are so closely linked [2].

1.1 Privacy Preserving Schemes in Smart Grid

Privacy is maintained in smart grids via a variety of strategies, including data aggregation and anonymization. In order to acquire fine-grained consumer energy usage data from smart metres, data aggregation is a common technique of doing so. MPC or homomorphic encryption is used to guarantee security and privacy needs are met during data aggregation. The MPC-based approaches enable several parties to collaboratively calculate a value as owned by individuals' data without revealing the substance of data with the other involved parties. When it comes to arithmetic calculations, homomorphic encryption-based approaches enable the same operation to be performed on encrypted text as it is on plaintext. Entities in the smart grid may do necessary calculations without understanding the data because of this characteristic. Using pseudonyms, hashing values, and other methods to obscure the actual identity of users is another common way to protect privacy in the smart grid [3]. Real-world consumers and their energy usage statistics are challenging to connect. As a result, a number of techniques are hybrid-based, which means they use more than one method to protect privacy. Similar approaches include temporal perturbation, Shamir's secret exchange, private keys and bit rotating methods [4].

1.2 Contribution

The main focus of the work is to design a method for smart grid that preserving privacy. This is done by using swarm intelligence algorithm. Sensitive data and the random key is read and XOR operation is performed between them for security purposes. The random key is generated using a JAYA algorithm based on the objective function. Here Entropy is taken as the objective function in the key generation method. The simulation analysis is done in MATLAB. According to the findings, the new approach outperforms the current ones.

1.3 Paper Organisation

The remaining paper is organized is as follows. Section 2 defines the related work. Section 3 illustrates the planned method is designed to provide privacy in the smart grid. Section 4 shows the simulation results of the planned method. In section 5 defines the conclusion and future scope.

2. Related Work

In this section, related work is shown to understand the existing encryption algorithms are deployed for security purposes.

Chen et al. [5],studied a fine-grained energy supply is possible due to the use of smart metres on the smart grid, which report power use to servers on a regular basis. There are, however, concerns about the privacy implications of the data that is routinely disclosed. They may, for instance, indicate whether or not the owner of the residence is at home and whether or not the television is operating. People are frightened of revealing this type of sensitive information since privacy is becoming a major concern. It was found that the conventional method continues to suffer from both a failure rate of the metres and an issue with their replacement in this study, so researchers came up with an idea for an improved method of collecting data from smart metres that relies on the noise addition method as well as an encryption algorithm called homomorphic. The experimental findings reveal that the calculation costs on both the aggregators and smart metre sides have been lowered after the simulations. Semantic security is shown through a powerful security analysis of the planned approach.

Barbosa et al. [6], There are numerous reasons for electricity companies to acquire high-resolution data on energy usage from consumers via a Smart Metering infrastructure. However, this data collecting entails a great deal of detail regarding the energy usage of the consumers being tracked. As a result, a critical issue must be addressed: how can consumers' privacy be protected while still allowing certain services to be provided? Clearly, there is a tradeoff between privacy and benefit in this situation. There are a variety of options for preserving privacy, but many of them have a negative impact on data effectiveness or are computationally costly. We suggest and analyse a lightweight strategy based on the inclusion of noise for privacy and utility in this study. We also discuss the impact of the technique in several Smart Grid situations using real customer data. Finally, we devise and test potential assaults on our solution.

ISSN 2322-0821 ISSN 2394-9910

International Research Journal of Engineering & Applied Sciences, IRJEAS
www.irjeas.org, ISSN(O): 2322-0821, ISSN(P): 2394-9910, Volume 10 Issue 2, Apr-Jun 2022, Page 23-32

Eibl et al. [7],studied that with smart metres, consumers are concerned about their privacy because of the extensive data collecting. To find a compromise between practicality and privacy, data from many smart metres may be combined. Differential confidentiality in smart metering has been presented as a way to ensure the privacy of end-users by perturbing aggregates. Due to this, the practicality of differential privacy for smart metering in the actual world cannot be assured. They examine the impact of differential privacy on actual smart metering data, with a particular focus on the need to strike a balance between utility needs and privacy concerns. It turns out that even with significant changes to the fundamental technique, an aggregation group of thousands of smart metres is still required to provide good usefulness.

Firorette et al. [8],Commercial and academic research may benefit greatly from high-fidelity energy networks. Since a result, these leaks create basic security and privacy issues, as they might disclose sensitive business information and reveal system flaws. For power networks in which transmission lines and transformer characteristics are obscured, this research examines ways to make the data available for analysis. Differential Privacy (DP), a framework that gives strong privacy assurances and has received a lot of attention recently, is used to accomplish this. Complex AC-infeasible networks are often the consequence of relying only on basic DP techniques. It is for this reason that this study proposes an innovative approach that ensures AC practicality while also preserving the authenticity of the obscured power network to some extent. In addition, the results of the experiments suggest that the obfuscation minimizes the potential harm from an attack carried out by exploiting the leaked dataset greatly.

Singh et al. [9], they have planned a privacy-preserving method for smart grid using ANU and noise addition method. In their work, the data is split into customer personal information and electricity consumption information. ANU algorithm is used for encrypt customer personal information and noise addition on electricity information by performing the perturbation algorithm. They achieved superior results in terms of execution time, avalanche effect, and memory consumption.

2.1 Motivation

In the literature, noise addition is done in the sensitive data to provide privacy. Noise addition is done by performing the data perturbation method, data encryption. However, generating a random key for data encryption is challenge. In this paper, a complete random key is generated using swarm intelligence algorithm by considering the objective function.

3. Planned Method

In this section, the planned privacy-preserving method is explained that is designed to secure smart meter data. Figure 1 shows the detail flowchart of the planned method. Initially, the smart meter dataset is read. When the dataset is pre-processed, sensitive attributes are separated from non-sensitive attributes, and the dataset is then divided again. The encryption algorithm is provided the information about the sensitive attributes. The encryption algorithm encrypts the sensitive attributes with the private key by performing the XOR operation and gives the encrypted sensitive data in the output. The private key is generated using the swarm intelligence algorithm. In the planned method, a JAYA algorithm is designed to generate a completely random key. After encryption, the encrypted sensitive data is concatenated with non-sensitive data. In the last, the performance of the planned method is analysed.

ISSN 2322-0821 ISSN 2394-9910

International Research Journal of Engineering & Applied Sciences, IRJEAS
www.irjeas.org, ISSN(O): 2322-0821, ISSN(P): 2394-9910, Volume 10 Issue 2, Apr-Jun 2022, Page 23-32

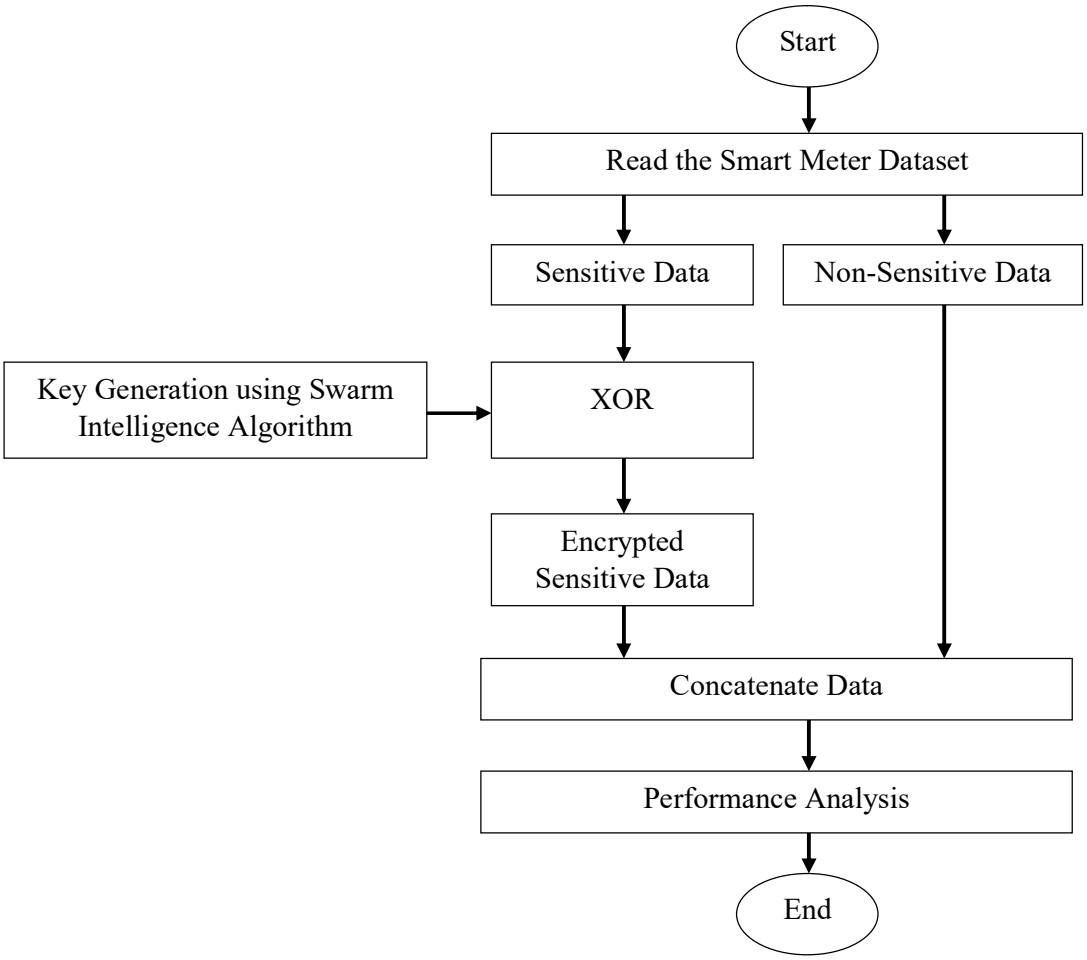

Figure 1 Flowchart of the planned privacy-preserving method

Next, a detailed description of the swarm intelligence algorithm is deployed for the planned method is explained.

3.1 JAYA Algorithm

At its inception, the JAYA method was designed to deal with optimization functions that were both complicated and unbounded [10]. Because it is derived from Sanskrit, the name JAYA literally translates as victory. Swarm-based intelligence and evolutionary algorithms are combined in this method, which is a population-based metaheuristic that incorporates the best qualities of both. As a result, it is inspired by natural phenomena such as the "survival of the fittest." This indicates that options in the JAYA population are also being drawn to the best global solutions while simultaneously ignoring the worst solutions. To put it another way, the selection procedure of the JAYA algorithm strives to come closer to success by finding the global best solutions, and it wants to avoid failure by racing away from the worst answers as fast as possible. Over other population-based techniques, the JAYA method has various benefits, including being simple to build and not requiring any algorithm-specific parameters (i.e., maximum number of iterations and the population size).

International Research Journal of Engineering & Applied Sciences, IRJEAS
www.irjeas.org, ISSN(O): 2322-0821, ISSN(P): 2394-9910, Volume 10 Issue 2, Apr-Jun 2022, Page 23-32

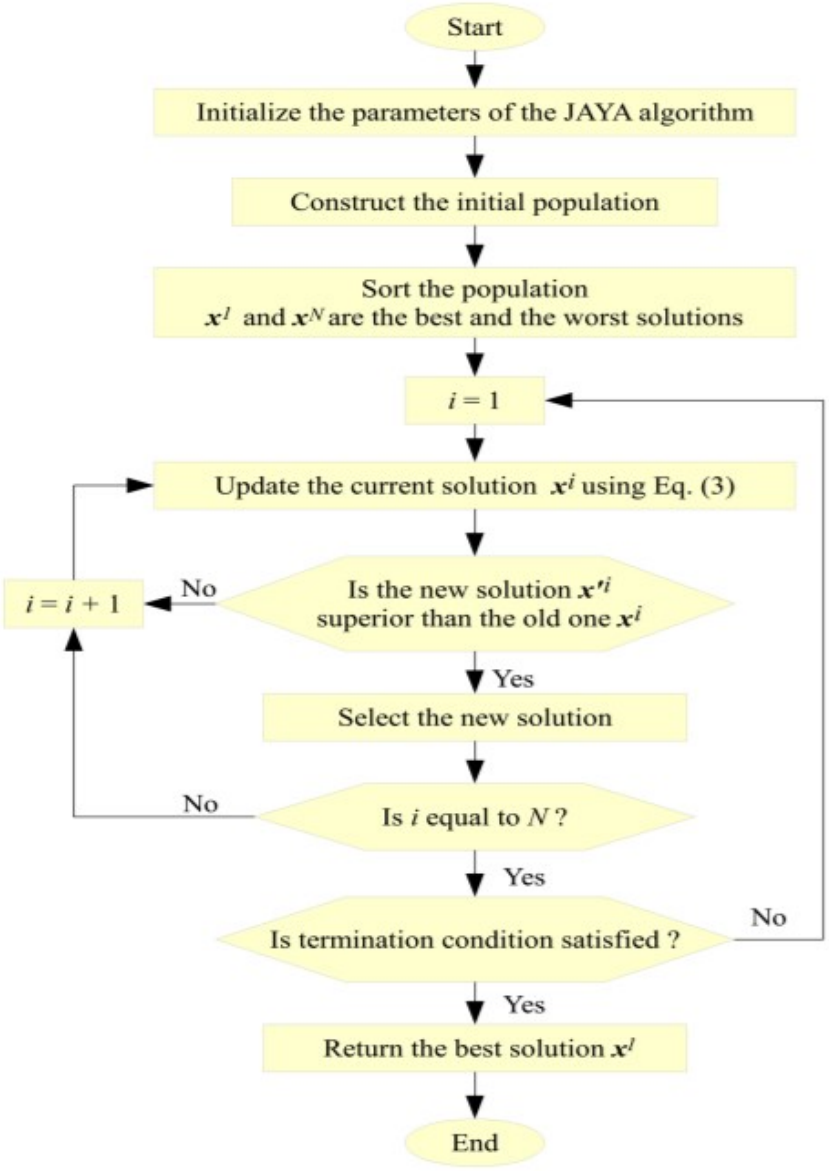

Figure 2 JAYA Algorithm [10]

The JAYA algorithm is comprised of six procedural phases. These procedural procedures may assist academics in the field of optimization algorithms in learning how to apply this method quickly and effectively. The flowchart in Fig. 2 depicts the processes involved in the JAYA algorithm's procedural steps. The pseudo-code for the JAYA algorithm is also given in Table 1.

ISSN 2322-0821 ISSN 2394-9910

International Research Journal of Engineering & Applied Sciences, IRJEAS
www.irjeas.org, ISSN(O): 2322-0821, ISSN(P): 2394-9910, Volume 10 Issue 2, Apr-Jun 2022, Page 23-32

Table 1 Pseudocode of JAYA Algorithm [10]

Algorithm 1 The pseudo-code of JAYA algorithm

Initialize the parameters of both JAYA algorithm and optimization problem (N, T, etc.).
Initialize a population of N solutions randomly.
Calculate $f(X_i)$ $\forall i = 1, 2, \ldots, N$
Sort the population: ($\boldsymbol{x}^1$ and $\boldsymbol{x}^N$ are the best and the worst solutions respectively).
t=1
while ($t \leq T$) **do**
  for $i = 1, \cdots, N$ **do**
    for $j = 1, \cdots, D$ **do**
      Set $r_1 \in$[0,1]
      Set $r_2 \in$[0,1]
      $x_j'^i = x_j^i + r_1 \times (x_j^1 - |x_j^i|) - r_2 \times (x_j^N - |x_j^i|)$
    end for
    if $f(\boldsymbol{x}'^i) \leq f(\boldsymbol{x}^i)$ **then**
      $\boldsymbol{x}^i = \boldsymbol{x}'^i$ {Update process}
    end if
  end for
  $t = t + 1$
end while

The procedure of JAYA algorithm is thoroughly discussed in following steps:

Step:1 JAYA method settings and optimization problem variables should be set to their default values at this point. The JAYA Algorithm's starting parameters are established at the run's beginning stage. No control parameters are required to use the algorithm JAYA. The population size N and the number of iterations T are the only two algorithmic parameters. Typically, an optimization issue is represented in this way:

$$\begin{aligned} &\min f(\boldsymbol{x}) \\ &\text{S.t.} \\ &g_j(\boldsymbol{x}) = c_j \quad \forall j = (1, 2, \ldots, n) \\ &h_k(\boldsymbol{x}) \leq d_k \quad \forall k = (1, 2, \ldots, m) \end{aligned} \tag{1}$$

where f(x) is the objective function used to determine the fitness of the solution x = (x1, x2,..., xD). where xi is a decision variable assigned a value between the minimum and maximum bounds such that xi ∈ [Xmini ,Xmaxi]. g_j is the j^{th} equality constraints and h_k is the k inequality constraints. Typically, the problem variables, dimensions, and associated data are taken from a reference dataset.

Step 2: Initial Population Construction for JAYA Algorithm:There are initial solutions (or populations) of JAYA algorithm that are built and saved in the JAYA Memory (JM). There are N solutions and D dimensions in Eq. 2, hence the JM is an augmented matrix of the size N x D, as stated in Eq. 2.Conventionally, solution is randomly constructed: JMi,j = Xmin j + (Xmin j − Xmax j) × rnd, ∀i∈ (1, 2, ⋯ , N) ⋀∀j ∈ (1, 2, ⋯ , D). The rnd function is a random generator and its value varies from 0 to 1.

$$\mathbf{JM} = \begin{bmatrix} x_1^1 & x_2^1 & \cdots & x_D^1 \\ x_1^2 & x_2^2 & \cdots & x_D^2 \\ \vdots & \vdots & \cdots & \vdots \\ x_1^N & x_2^N & \cdots & x_D^N \end{bmatrix} \begin{bmatrix} f(\boldsymbol{x}^1) \\ f(\boldsymbol{x}^2) \\ \vdots \\ f(\boldsymbol{x}^N) \end{bmatrix} \tag{2}$$

As a result, the JM solutions are ranked in ascending order based on their objective function values for each solution. Therefore, x^1 is the best answer, while x^N is the worst.

Step: 3 Evaluation Process of JAYA Algorithm: Using the JAYA operator given in Eq. 3, the decision variables of all JM solutions are modified iteratively.

$$x_j'^i = x_j^i + r_1 \times (x_j^1 - |x_j^i|) - r_2 \times (x_j^N - |x_j^i|) \tag{3}$$

In Eq. (3), $x_j'^i$ and x_j^i denotes the new updated and current solution. On the the hand, r1 and r2 are two uniform function and its values varies in the range

ISSN 2322-0821 ISSN 2394-9910

International Research Journal of Engineering & Applied Sciences, IRJEAS
www.irjeas.org, ISSN(O): 2322-0821, ISSN(P): 2394-9910, Volume 10 Issue 2, Apr-Jun 2022, Page 23-32

of [0-1]. In order to find the correct balance between exploitation and exploration, these produced random numbers are employed. x1 j is the best solution's decision variable j, whereas xN j is the worst solution's decision variable j. For the JAYA algorithm, the distance between the best solution's decision variables and the present one, and the gap among optimal solution's model parameters and current one, determines the diversity control. Higher exploitation occurs at a closer distance, whereas exploration occurs at a greater distance [11-12].

Step4: Update JM: Every iteration, the JM solutions will be updated. Calculate the objective function value of the new solution f(x'i). If f(x'i) f, the current solution xi will be replaced by the new solution x′i (xi). This procedure will be repeated N times.

Step: 5 Stop rule. In order to achieve the stopping rule, which in certain cases is the maximum number of iterations T, the JAYA algorithm repeats Steps 3 and 4 continuously.

4. Simulation Results

The planned method is simulated in MATLAB. Further, various performance metrics are calculated for it, as explained below.

4.1 Mean Square Error (MSE):This parameter is used to measured the error between original and encrypted data. It is calculated using the following equation.

$$MSE = \frac{\sum_{i=1}^{M}(O_i - E_i)^2}{M} \quad (4)$$

Table 2 shows the MSE value for different files are taken under consideration for the planned method.

Table 2 MSE for the Planned Method

Files	MSE
File1	6701
File2	3066.3
File3	6764.6
File4	5057.2
File5	7529.6

4.2 Peak Signal to Noise Ratio (PSNR):Peak Signal-to-Noise Ratio (PSNR) is utilized to highlight the differences between the original and encrypted data. The primary benefit of employing this measurement is determining the noise level of encrypted data. The PSNR values of the provided data are calculated using the following equation:

$$PSNR = 10\log_{10}\frac{P^2}{MSE} \quad (5)$$

In encryption scheme, low value of PSNR is desirable. Table 3 shows the PSNR value for different files are taken under consideration for the planned method. The result shows that the planned method achieves low PSNR.

Table 3 PSNR for the Planned Method

Files	PSNR
File1	9.8694
File2	13.2647
File3	9.8284
File4	11.0917
File5	9.3631

4.3 Correlation Coefficient (CC): correlation coefficient parameter is used to estimate the encrypted data quality. The correlation coefficient value varies from -1 to 1. The 1 value reflects the high correlation between original and encrypted data whereas 0 value reflects the low correlation coefficient between data. In the encryption scheme, low value of correlation coefficient is desirable. Table 4 shows the correlation coefficient value for different files are taken under consideration for the planned method. The result shows that the planned method achieve correlation coefficient near 0 value.

Table 4 Correlation Coefficient for the Planned Method

ISSN 2322-0821 ISSN 2394-9910

International Research Journal of Engineering & Applied Sciences, IRJEAS
www.irjeas.org, ISSN(O): 2322-0821, ISSN(P): 2394-9910, Volume 10 Issue 2, Apr-Jun 2022, Page 23-32

Files	CC
File1	-0.0675
File2	0.1716
File3	-0.0064
File4	0.0159
File5	-0.3565

4.4 Convergence Graph

The convergence graph is plotted between fitness function vs. iteration. In the planned method, random key is generated using JAYA algorithm. The convergence graph for the key generation is shown in Figure 3. The result shows that the planned method gives approximate 1 entropy in the 23rd iteration.

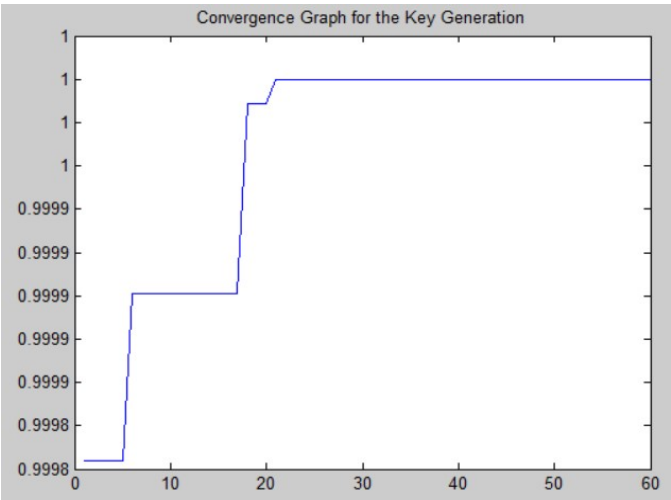

Figure 3 Convergence Graph

4.5 Key Generation Tests: In the literature, a number of key generation test is available. In this work, I have calculated the frequency test. The frequency test calculates the 0's and 1's probability in the generated key. In the ideal case, 50% 0's and 1's required in the key. Table 5 shows the generated keys. The result shows that the planned method generates approximate equal number of 0's and 1's.

Table 5 Generated Keys

Generated Keys	0's and 1's Probability
[162 119 0 94 183 176 68 88 227 63 238 66 178 49 177 63 136 133 157 218 66 57 82 195 162 187 77 2 232 179 32 231 96 154 5 132 30 237 106 216 186 164 187 194 247 229 252 57 199 104 197 221 250 55 192 154 140 170 208 183 129 109 167 94]	0's=255 1's=257
[223 192 13 216 46 137 233 119 140 79 168 254 74 19 3 95 100 231 177 193 249 247 18 232 15 5 31 137 200 182 30 10 103 42 233 213 247 199 33 125 214 112 28 148 210 70 233 95 39 92 102 136 179 64 32 171 104 240 147 47 179 72 113 163]	0's=256 1's=256

4.6 Comparative Analysis

ISSN 2322-0821 ISSN 2394-9910

International Research Journal of Engineering & Applied Sciences, IRJEAS
www.irjeas.org, ISSN(O): 2322-0821, ISSN(P): 2394-9910, Volume 10 Issue 2, Apr-Jun 2022, Page 23-32

In this section, the planned method is compared with the existing method [9] based on the correlation and execution time parameter in Table 6 and 7.

The result shows that the planned method provides lesser correlation coefficient when compared to data perturbation method whereas approximate same correlation coefficient as compared to ANU algorithm. On other hand, Table 7 shows that the planned method takes lesser execution time for data encryption over the existing method.

Table 6 Comparative Analysis based on Correlation Parameter

Files	Singh et al. [9]		Planned Method
	ANU Algorithm	Data Perturbation	
File1	-0.0687	-0.6074	-0.0675
File2	-0.1574	-0.6090	0.1716
File3	-0.0662	-0.6079	-0.0064
File4	-0.1505	0.6108	0.0159
File5	-0.1276	-0.6089	-0.3565

Table 7 Comparative Analysis based on Execution Time

	Singh et al. [9]	Planned Method
Execution Time (in seconds)	0.42	0.185

5. Conclusion and Future Work

In this paper, a privacy-preserving method is designed for smart grid. To achieve this goal, the smart meter dataset is split into sensitive and non-sensitive part. The sensitive part is encrypted by performing XOR operation with a random key. The random key is generated using the JAYA algorithm. Based on the objective function a completely random key is generated by using JAVA algorithm. The performance analysis is done using various parameters such as MSE, PSNR, correlation, and key generation tests. The result shows that the planned method provides lower PSNR and correlation coefficient between original and encrypted data. Besides that, the planned method provides superior results over the existing methods. In the future, the dataset is post-process for load forecasting and bill generation purposes.

References

[1] Lawal, M.A. and Hassan, S.R., 2021. Privacy Preservation in Smart Grid Environment. In *Research Anthology on Privatizing and Securing Data* (pp. 1392-1410). IGI Global.

[2] Syed, D., Refaat, S.S. and Bouhali, O., 2020. Privacy Preservation of Data-Driven Models in Smart Grids Using Homomorphic Encryption. *Information*, *11*(7), p.357.

[3]Patil, S., Joshi, S. and Patil, D., 2020. Enhanced privacy preservation using anonymization in IoT-enabled smart homes. In *Smart Intelligent Computing and Applications* (pp. 439-454). Springer, Singapore.

[4]Olakanmi, O.O., 2017. Secure and privacy-oriented obfuscation scheme for smart metering in smart grid via dynamic aggregation and lightweight perturbation. *International Journal of Information Privacy, Security and Integrity*, *3*(1), pp.38-57.

[5]Chen, Y., Martínez, J.F., Castillejo, P. and López, L., 2018. A privacy-preserving noise addition data aggregation scheme for smart grid. *Energies*, *11*(11), p.2972.

[6] Barbosa, P., Brito, A., Almeida, H. and Clauß, S., 2014, March. Lightweight privacy for smart metering data by adding noise. In *Proceedings of the 29th Annual ACM Symposium on Applied Computing* (pp. 531-538).

[7] Eibl, G. and Engel, D., 2017. Differential privacy for real smart metering data. *Computer Science-Research and Development*, *32*(1-2), pp.173-182.

[8] Fioretto, F., Mak, T.W. and Van Hentenryck, P., 2019. Differential privacy for power grid obfuscation. *IEEE Transactions on Smart Grid*, *11*(2), pp.1356-1366.

ISSN 2322-0821 ISSN 2394-9910

[9] Singh, R. and Jain, P. (2020). Lightweight privacy-preserving scheme for the smart grid data using ANU and Perturbation Algorithm. *International Journal of Advance Research, Ideas and Innovations in Technology*, [online] 6(4), pp.267–272. Available at: https://www.ijariit.com/manuscript/lightweight-privacy-preserving-scheme-for-the-smart-grid-data-using-anu-and-perturbation-algorithm/ [Accessed 2 Jun. 2022].

[10] Zitar, R.A., Al-Betar, M.A., Awadallah, M.A., Doush, I.A. and Assaleh, K., 2021. An intensive and comprehensive overview of jaya algorithm, its versions and applications. *Archives of Computational Methods in Engineering*, pp.1-30.

[11] Berlin, K. and Padmapriya, A., 2014. Performance Analysis of Threshold based Image Encryption. *International Journal of Computer Applications*, *975*, p.8887.

[12] Sethi, N. and Vijay, S., 2013, April. Comparative image encryption method analysis using new transformed-mapped technique. In *Conference on advances in communication and control systems (CAC2S)* (pp. 46-50).

ISSN 2322-0821 ISSN 2394-9910